Steiner loops of nilpotency class 2

A. Grishkov, D. Rasskazova, M. Rasskazova, I. Stuhl

Abstract

We describe Steiner loops of nilpotency class two.

1 Introduction and Preliminaries

A *loop* is a set L with a binary operation $\cdot$ and a neutral element $1 \in L$, such that for every $a, b \in L$ the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions.

The *center* of a loop L is an associative subloop $Z(L)$ consisting of all elements of L which commute and associate with all other elements of L. A loop L is *nilpotent* if the series L, $L/Z(L)$, $[L/Z(L)]/Z[L/Z(L)]$ ... terminates at 1 in finitely many steps. In particular, L is of *nilpotency class two* if $L/Z(L) \neq 1$ and $L/Z(L) \neq 1$ is an abelian group. For $x, y, z \in L$, define the *associator* (x, y, z) of x, y, z by $(xy)z = (x(yz))(x, y, z)$. The *associator subloop* $A(L)$ of L is the smallest normal subloop H of L such that L/H is a group. Thus, $A(L)$ is the smallest normal subloop of L containing associators (x, y, z) for all$x, y, z \in L$.

A *Steiner triple system* is an incidence structure consisting of points and blocks such that every two distinct points are contained in precisely one block and any block has precisely three points. A finite Steiner triple system with n points exists if and only if $n \equiv 1$ or 3 (mod 6) (cf. [6], V.1.9 Definition).

A Steiner triple system $\mathfrak{S}$ provides a multiplication on pairs of different points x, y taking as product the third point of the block joining x and y. Defining $x \cdot x = x$, we get a *Steiner quasigroup* associated with $\mathfrak{S}$. Adjoining an element e with $ex = xe = x$, $xx = e$, we obtain a Steiner loop S, see below. Conversely, a Steiner loop determines a Steiner triple system whose points are the elements of $S \setminus e$, and the blocks are triples $\{x, y, xy\}$ where $x, y \in \mathfrak{S}$, $x \neq y$.

2010 *Mathematics Subject Classification:20N05, 05B07.*

Key words and phrases: Steiner triple systems, Steiner loops, nilpotency index 2

A totally symmetric loop of exponent 2 is called *Steiner loop.* Steiner loops form a Schreier variety; it is precisely the variety of all diassociative loops of exponent 2. Steiner loops are in a one-to-one correspondence with Steiner triple systems (see in [2] p. 310).

Since Steiner loops form a variety, we can deal with free objects. Moreover, according to [3], we have the following. Let $\mathtt{X}$ be a finite ordered set and let $W(\mathtt{X})$ be a set of non-associative $\mathtt{X}$-words. The set $W(\mathtt{X})$ has an order, $>$, such that $v > w$ if and only if $|v| > |w|$ or $|v| = |w| > 1$, $v = v_1v_2$, $w = w_1w_2$, $v_1 > w_1$ or $v_1 = w_1, v_2 > w_2$. Next, we define the set $S(\mathtt{X})^* \subset W(\mathtt{X})$ of S-words by induction upon the length of word:

- $\mathtt{X} \subset S(\mathtt{X})^*$,
- $wv \in S(\mathtt{X})^*$ precisely if, $v, w \in S(\mathtt{X})^*$, $|v| \le |w|$, $v \ne w$ and if $w = w_1 \cdot w_2$, then $v \ne w_i$, $(i = 1, 2)$.

On $S(\mathtt{X}) = S(\mathtt{X})^* \cup \{\emptyset\}$ we define a multiplication (still denoted by $\cdot$) in the following manner:

1. $v \cdot w = w \cdot v = vw$ if $vw \in S(\mathtt{X})$,
2. $(vw) \cdot w = w \cdot (vw) = w \cdot (wv) = (wv) \cdot w = v$,
3. $v \cdot v = \emptyset$.

A word $v(x_1, x_2, ..., x_n)$ is *irreducible* if $v \in S(\mathtt{X})^*$. The set $S(\mathtt{X})$ with the multiplication as above is a free Steiner loop with the set of free generators $\mathtt{X}$.

In what follows we discuss Steiner loops of nilpotency class 2.

2 Centrally nilpotent Steiner loops of class 2

Let $S(\mathtt{X}) > S_1(\mathtt{X}) > S_2(\mathtt{X}) > ...$ be a central series of the free Steiner loop $S(\mathtt{X})$ with free generators $\mathtt{X} = \{x_1, ..., x_n\}$. Then $V = S(\mathtt{X})/S_1(\mathtt{X})$ is an $\mathbf{F}_2$-space of dimension $n := |\mathtt{X}|$. Given $\sigma = \{i_1 < i_2 < ... < i_s\} \subseteq I_n$ define the corresponding element $\sigma = (((x_{i_1}x_{i_2})x_{i_3})...x_{i_s})$ of $S(\mathtt{X})$. Hence $\{\sigma | \sigma \subseteq I_n\}$ is a set of representatives of $S(\mathtt{X})/S_1(\mathtt{X})$. Determine a set of representatives of $Z = S_1(\mathtt{X})/S_2(\mathtt{X})$.

Set L_f be a central extension of $\mathbf{F}_2$-spaces V and Z in the variety of Steiner loops. It is well known that L_f is a central f-extension of Z by V if and only if L_f is isomorphic to a loop defined on $V \times Z$ by the multiplication

$$(v_1, z_1) \circ (v_2, z_2) = (v_1 + v_2, f(v_1, v_2) + z_1 + z_2). \tag{1}$$

Here $f : V \times V \longrightarrow Z$ is a cocycle, that is, a map satisfying

$$f(0, v_1) = 0,\ f(v_1, v_1) = 0,\ f(v_1, v_2) = f(v_2, v_1),\ f(v_1+v_2, v_2) = f(v_1, v_2) \quad (2)$$

for all $v_1, v_2 \in V$. Denote by $Z^2(V, Z)$ the set of all cocycles. Next, let $C^1(V, Z)$ be the set of all functions $g : V \longrightarrow Z$ and $\delta : C^1(V, Z) \longrightarrow Z^2(V, Z)$ such that

$$\delta(g)(v_1, v_2) = g(v_1 + v_2) + g(v_1) + g(v_2).$$

for all $v_1, v_2 \in V$. Let

$$B^2(V, Z) = \delta(C^1(V, Z))$$

and

$$H^2(V, Z) = Z^2(V, Z)/B^2(V, Z).$$

Lemma 1 *Central extensions L_{f_1} and L_{f_2} corresponding to different cocycles f_1 and f_2 are isomorphic if and only if $f_1 = f_2$ in $H^2(V, Z)$.*

Proof. The map $\varphi = (\varphi_1, \varphi_2) : L_{f_1} \longrightarrow L_{f_2}$, with $\varphi_1(v, z) = v$ and $\varphi_1(v, z) = z + g(v)$, determines an isomorphism if and only if $f_1(v_1, v_2) = f_2(v_1, v_2)+g(v_1+v_2)+g(v_1)+g(v_2)$, i.e., $f_1 = f_2$ in $H^2(V, Z)$. This is because

$$\varphi((v_1, z_1) \circ (v_2, z_2)) = (v_1 + v_2, f_1(v_1, v_2) + z_1 + z_2 + g(v_1 + v_2)) =$$

$$(v_1 + v_2, f_2(v_1, v_2) + z_1 + z_2 + g(v_1) + g(v_2)) = \varphi(v_1, z_1) \circ \varphi(v_2, z_2).$$

■

Let $\{v_1, ..., v_n\}$ be a basis of V over $\mathbf{F}_2$; as usually, we can identify V with P_n - the set of all subsets of I_n. Consider a subset $Z_0^2(V, Z) \subset Z^2(V, Z)$, where $f \in Z_0^2(V, Z)$ if and only if $f(\sigma, i) = 0$, $i > \max(\sigma)$, $\sigma \in P_n = V$.

Lemma 2 $Z^2(V, Z) = Z_0^2(V, Z) \oplus B^2(V, Z)$.

Proof. First, consider the case when $f \in Z_0^2(V, Z) \cap B^2(V, Z)$ Then $f = \delta(g)$, and for any $\sigma \in P_n$ and i such that $i > \max(\sigma)$ we have

$$f(\sigma, i) = g(\sigma \cup i) + g(\sigma) + g(i) = 0.$$

Then $g(\sigma) = \sum_{i \in \sigma} g(i)$. Hence,

$$f(\sigma, \tau) = g(\sigma \triangle \tau) + g(\sigma) + g(\tau) = \sum_{i \in \sigma \triangle \tau} g(i) + \sum_{i \in \sigma} g(i) + \sum_{i \in \tau} g(i)$$

$$= \sum_{i \in \sigma \setminus \tau} g(i) + \sum_{i \in \tau \setminus \sigma} g(i) + \sum_{i \in \sigma \cap \tau} g(i) + \sum_{i \in \sigma \setminus \tau} g(i) + \sum_{i \in \tau \cap \sigma} g(i) + \sum_{i \in \tau \setminus \sigma} g(i) = 0.$$

Now, suppose $f \in Z^2(V,Z)$. For $\sigma = (i_1, ..., i_k)$ we define $\sigma^s = (i_1, ..., i_{s-1})$, $s > 1$, and $g(\sigma) = \sum_{s=2}^{k} f(\sigma^s, i_s)$, assuming $|\sigma| > 1$, $g(i) = 0$. Then $f + \delta(g) \in Z^2{}_0(V,Z)$. Indeed, if $i = i_{k+1} > i_k = \max(\sigma)$ then

$$(f + \delta(g))(\sigma, i) = f(\sigma, i) + g(\sigma \cup i) + g(\sigma) + g(i)$$

$$= f(\sigma, i) + \sum_{s=2}^{k+1} f(\sigma^s, i_s) + \sum_{s=2}^{k} f(\sigma^s, i_s) = 0,$$

as $\sigma^{k+1} = \sigma$ and $i_{k+1} = i$. This yields that $f + \delta(g) \in Z^2{}_0(V,Z)$ completing the proof of the lemma. ∎

We call a pair (σ, τ) *regular* if and only if $|\sigma| + |\tau| < |\sigma| + |\sigma \triangle \tau|$ and $|\sigma| + |\tau| < |\tau| + |\sigma \triangle \tau|$ or $|\sigma| + |\tau| = |\sigma| + |\sigma \triangle \tau|$ but $\min(\sigma \triangle \tau) < \min(\tau \setminus \sigma)$. (Here and below $\triangle$ stands for the set-theoretical difference.) Note, that if $\emptyset \neq \sigma \neq \tau \neq \emptyset$ then precisely one of the pairs $(\sigma, \sigma\triangle\tau)$, (σ, τ), $(\sigma\triangle\tau, \tau)$ is regular. A regular pair is called *strongly regular* if $|\sigma| \geq |\tau| > 1$ or $|\sigma| \geq |\tau| = 1$ but $i < \max(\sigma)$, where $\tau = \{i\}$.

Lemma 3 *The number of elements of the set of all non-ordered strongly regular pairs* (σ, τ) *is*

$$\frac{1}{3}(2^{2n-1} + 1) - 3 \cdot 2^{n-1} + n + 1.$$

Proof. Let P be the set of all non-ordered pairs (σ, τ). Then $P = P_0 \cup P_1$, where $P_0 = \{(\sigma, \sigma) | \sigma \subseteq I_n\}$ and $P_1 = \{(\sigma, \tau) | \sigma \neq \tau \subseteq I_n\}$. Then $P_1 = P_2 \cup P_3$ where $P_2 = \{(\sigma, \emptyset) | \emptyset \neq \sigma \subseteq I_n\}$, $P_3 = \{(\sigma, \tau) | \tau \neq \sigma \neq \emptyset \subseteq I_n\}$. It is easy to see that pairs $(\sigma\triangle\tau, \tau)$ and $(\sigma\triangle\tau, \sigma)$ are contained in $P_0 \cup P_2$ or in P_3 if (σ, τ) is contained in $P_0 \cup P_2$ or in P_3, respectively. Since $|P_1| = 2^{n-1}(2^n - 1)$, $|P_2| = 2^n - 1$ and $P_2 \cap P_3 = \emptyset$, we get that $|P_3| = (2^n - 1)(2^{n-1} - 1)$. It means that the number of regular pairs equals $\frac{1}{3}(2^n - 1)(2^{n-1} - 1)$.

If pair (σ, τ) is regular but not strongly regular then $\tau = \{i\}$, $i > max(\sigma)$. Hence, for a given i we have exactly $(2^{i-1} - 1)$ regular but not strongly regular pairs. Then the number of strongly regular pairs equals

$$\frac{1}{3}(2^n - 1)(2^{n-1} - 1) - \sum_{i=2}^{n}(2^{i-1} - 1)$$

$$= \frac{1}{3}(2^n - 1)(2^{n-1} - 1) - 2^n + n + 1$$

$$= \frac{1}{3}(2^{2n-1} + 1) - 3 \cdot 2^{n-1} + n + 1.$$

∎

Theorem 4 *The union of sets*

$$\{(i, \sigma \setminus i, \tau) | (\sigma, \tau) \ \textit{strongly regular}\ \sigma \cap \tau = \emptyset, i = max(\sigma \cup \tau)\}$$

and

$$\{(i, \sigma, \tau) | (\sigma, \tau) \ \textit{strongly regular}, \ \ i = max(\sigma \cap \tau)\}.$$

is a basis of $\mathbf{F}_2$*-space* $S_1(\mathtt{X})/S_2(\mathtt{X})$*,*

Moreover,

$$\dim_{\mathbf{F}_2}(S_1(\mathtt{X})/S_2(\mathtt{X})) = \frac{1}{3}(2^{2n-1}+1) - 3 \cdot 2^{n-1} + n + 1,$$

where $n := |\mathtt{X}|$*.*

Proof. We have the following relation involving associators:

$$(\sigma, \mu, \tau) = f(\sigma, \mu) + f(\mu, \tau) + f(\sigma \triangle \mu, \tau) + f(\sigma, \mu \triangle \tau). \tag{3}$$

Let (σ, τ) be a strongly regular pair, with $|\sigma| \geq |\tau|$. We will use induction in $r := |\sigma| + |\tau|$ and set $i = max(\sigma \cup \tau) \in \sigma$. Then by virtue of (3) we obtain

$$(i, \sigma \backslash i, \tau) = f(i, \sigma \backslash i) + f(\sigma \backslash i, \tau) + f(\sigma, \tau) + f(i, (\sigma \backslash i) \triangle \tau)$$

$$= f(\sigma \backslash i, \tau) + f(\sigma, \tau).$$

Furthermore, by induction set $P_0 = \{(i, \sigma \backslash i, \tau) | (\sigma, \tau) - \text{strongly regular}, \sigma \cap \tau = \emptyset\}$ forms a basis of $Q := \{f(\sigma, \tau) | (\sigma, \tau) - \text{strongly regular}, \sigma \cap \tau = \emptyset\}$.

Set $P_1 = \{(i, \sigma, \tau) | (\sigma, \tau) - \text{strongly regular}, i = \max(\sigma \cap \tau \neq \emptyset)\}$ then P_1 is a basis of Q. ■

Note that there are exactly 80 non-isomorphic Steiner triple systems of order 15. Moreover, there is only one nilpotent non-associative Steiner loop S_{16} of order 16 (cf. [5]), and it corresponds to the system N.2 in [4] p. 19. Furthermore, S_{16} has the GAP code SteinerLoop(16, 2); the label 2 indicates the system order as in the list established in monograph [1].

Take $S_N(\mathtt{X})$ where $\mathtt{X} = \{x_1, x_2, x_3\}$ is the 3-generated free Steiner loop of nilpotency class 2 and let $Z = \langle (z_1, z_2, z_3) \rangle$ be a center of $S_N(\mathtt{X})$. Then $S_{16} = S_N(\mathtt{X})/Z_0$, where $Z_0 \subset Z = \langle (z_1, z_2, z_3) \rangle$ is an elementary abelian 2-group of order 4. Moreover, $\mathrm{Aut}(S_N(\mathtt{X})) = GL_3(\mathbf{F}_2) \cdot \mathcal{Z}$ where $\mathcal{Z} = \langle \varphi : x_i \longrightarrow x_i t_i \rangle$, $t_i \in Z$, $(i = 1, 2, 3)$. Since $GL_3(\mathbf{F}_2)$ acts transitively on the set of all 2-dimensional $\mathbf{F}_2-$subspaces of $Z \simeq \mathbf{F}_2^3$, there exists a unique factor loop $S_N(\mathtt{X})/Z_0$, where Z_0 is an elementary abelian 2-group of order 4. This fact confirms that there exists a unique nilpotent non-associative Steiner loop of order 16.

Acknowledgement

A. Grishkov is supported by FAPESP, CNPQ (Brazil) and RFFI Grants 13-01-00239, 2014/319-258 (Russia) and expresses his gratitude. I. Stuhl is supported by FAPESP Grant - process number 11/51845-5, and expresses her gratitude to IMS, University of São Paulo, Brazil and to Math Dept, University of Denver for the warm hospitality.

References

[1] Ch. J. Colbourn, A. Rosa, Triple systems, *Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, (1999).*

[2] B. Ganter, U. Pfüller, A remark on commutative di-associative loops, *Algebra Universalis, 21, (1985), 310 – 311.*

[3] A. Grishkov, D. Rasskazova, M. Rasskazova, I. Stuhl, Free Steiner triple systems and their automorphism groups, *Journal of Algebra and its Applications, 14, (2015)*

[4] R. A. Mathon, K. T. Phelps, A. Rosa, Small Steiner triple systems and their properties, *Ars. Combinatoria, 15, (1983), 3 – 110.*

[5] G. P. Nagy, P. Vojtěchovský, Loops: Computing with quasigroups and loops in GAP, *version 2.2.0, available at http://www.math.du.edu/loops*

[6] H. O. Pflugfelder, Quasigroups and Loops: Introduction, *Heldermann Verlag, Berlin (1990).*

Alexander Grishkov
Institute of Mathematics and Statistics
University of São Paulo
05508-090 São Paulo, SP, Brazil
E-mail: *grishkov@ime.usp.br*

Diana Rasskazova
Institute of Mathematics and Statistics
University of São Paulo
05508-090 São Paulo, SP, Brazil

E-mail: *ivakirja@ime.usp.br*

Marina Rasskazova
Omsk Service Institute
644099 Omsk, Russia
E-mail: *marinarasskazova1@gmail.com*

Izabella Stuhl
IMS, University of São Paulo
05508-090 São Paulo, SP, Brazil
Math Dept, University of Denver
Denver, CO 80208 USA
University of Debrecen
H-4010 Debrecen, Hungary
E-mail: *izabella@ime.usp.br*